Remarks

The Office Action mailed August 6, 2003, has been carefully reviewed and the foregoing amendment has been made in consequence thereof.

Claims 1, 3-17, 19-26, and 28 are pending in this application. Claims 1, 3-17, 19-26, and 28 stand rejected.

The rejection of Claims 1, 3-17, 19-26, and 28 under 35 U.S.C. § 103 as being unpatentable over Goldhaber et al. (U.S. Patent No. 5,855,008) in view of Kepecs (U.S. Patent No. 6,009,411) is respectfully traversed.

Goldhaber et al. describe a system for brokering the attention of consumers (see Column 4, lines 46-50). The system uses a database of digitally stored electronic demographic profiles of potential viewers (members), the databases are private, dynamic and interactive. The system is configured to protect member privacy, while at the same time maintaining personal information files that permit specialized targeting of ads (See Column 6, lines 30-35). Referring to Column 7, lines 2-5 of Goldhaber et al., it is indicated that an advertiser may pay for consumer names and addresses. Further, it is indicated at Column 12, line 45 to Column 13, line 13, that name, address, and telephone data is required from an individual (member) when generating a consumer database. Therefore, while Goldhaber et al. describe profile data (i.e. Gender, Age, Ethnicity) as being separate from personal data (i.e. name, address, and telephone), all are required and stored in the described database. To emphasize the point, attention is directed to Column 13, lines 28-30 where it states that the personal data, i.e. contact "information provided by the consumer is stored in the contact information block (122) of the database." Such entry and storage of contact information is not indicative of anonymous data sets, nor indicative of any system which has data sets which do not include names, addresses, and social security numbers of individual participants. Certainly the acquisition of such information as described in Goldhaber et al. is not indicative of a method that maintains the anonymity of an individual through an inability to accept contact information in the profile.

Kepecs describes a method and system for distributing and redeeming electronic promotions to a consumer through the Internet. see Abstract. An account is maintained for each consumer and a unique key is associated with each consumer account. This account may be established by a registration process. Access is permitted to the consumer account upon presentation of the unique key over the communications network. The consumer is presented discount choices of items available in at least one store associated with the unique key. Upon purchase of items at the associated store by the consumer, such data are received, and the selections and purchases are reconciled to record a credit in the consumer account. No direct consumer identification is maintained in the consumer account to preserve the anonymity of the consumer. For example, only the loyalty card identifier is managed, therefore, the identity of the consumer is not needed. Column 2, lines 33-54.

A unique Key identifies the account of each consumer, but not necessarily the actual identity of the consumer. Column 5, lines 55-57. The Keys are in a database, and the Key Database may contain alternatively or concurrently some other personal identification, such as a Social Security number, a driver license number, passport number, or even biometric information, such as a fingerprint, of the consumer. Finally, the lowest level of identification is simply the KEY with no other identification data. This method may be used by the DAP computer 11 even if the KEY has non-anonymous bindings elsewhere (for example, if the KEY is associated with a store's loyalty card). Thus, the consumer can still be anonymous to the DAP, even if the store is aware of the consumer's identity or just his address. Column 6, lines 22-59.

The KEY described in Kepecs still appears to be generated by computer systems that are networked to other computer systems, which by their nature would include contact information. For example, at Column 4, lines 7-9, Kepecs describes that the "consumer may ... receive a credit in a designated financial account, e.g., the consumer's credit card account." Also at Column 5, lines 40-44, the "connection allows credit obtained by the purchase of discounted goods to be placed into the consumer's account at the consumer's financial institution...". Further, at Column 5, lines 54-55, Kepecs states that DAP computer 11 maintains a Key Database of the consumers'

accounts, each identified by a unique key. However, at Column 5, lines 28-45, interconnections of the DAP computer 11 to other computer systems are described. Specifically, the general network interconnection of the DAP computer 11, not only with the DAP Internet server 14 and master store computer 23, but also with the computer 31 of a discounter (DIS) and a computer 32 of the discounter's financial institution (DISFIT) is illustrated. The connection to the DIS computer 31 allows the DAP computer 11 to receive discount information, detailed below, from the discounter. The DAP computer 11 communicates with the DISFIT computer 32 so that the discounter's account is debited for goods purchased by the consumers under the discounter's discount. The DAP computer 11 may also be connected to the computer 24 of the consumer's financial institution (CONFIT). This connection allows credits obtained to be placed into the consumer's account at the consumer's financial institution as described above.

Further, at Column 5, lines 47-50, the DAP computer 11 is connected to this network and other private networks belonging to the financial institutions of the consumers. The system described by Kepecs does not provide complete anonymity to a consumer, since the KEY has non-anonymous bindings elsewhere. In other words, a consumer may only need to utilize their key to "anonymously" identify themselves to the DAP computer 11, but DAP computer 11 is networked to other computers which bind the KEY to contact information to allow for the crediting and debiting of accounts as described above and throughout the Kepecs patent. Therefore, although the key is anonymous, once a user accesses the system with the KEY, the system of Kepecs is able to identify the user due to the contact information which the computer has access to (e.g. the other computers described as being networked to DAP computer 11).

Claim 1 recites a method for prompting an individual to create an anonymous data profile for the individual. The method includes the steps of "providing the individual with access to a database," "requesting anonymous profile information, about the individual be entered into the database," "maintaining the anonymity of the individual through an inability to accept contact information in the profile" and "compensating the individual for either or both of entry of the anonymous profile information and feedback provided in response to marketing data."

While, both Goldhaber et al. and Kepecs attempt to protect contact information, it appears that neither possess an inability to accept contact information. The selection of only a KEY with no other identification data does not imply an inability to accept contact information. It appears that the system of Kepecs does have an ability to accept contact information by virtue of the ability to accept the personal information listed above. The disclosure of Kepecs certainly describes a computer that attempts to maintain anonymity, through utilization of the stand-alone KEY, but admits that such computer maintains non-anonymous bindings utilizing the KEY to identify the consumer to other computers as above described. Further, in the embodiment where the KEY is utilized alone, it appears to be the choice of the consumer to utilize the KEY solely, and not an implementation of a method which includes an inability to accept contact information.

Goldhaber et al. in view of Kepecs do not describe nor suggest a method for creating an anonymous profile for an individual that includes "an inability to accept contact information". For example, Goldhaber et al. describe a system which requires both personal data (contact information) and profile data to be entered by a user. In addition, Goldhaber et al. describe that the personal data can be obtained by outside entities, should the member agree to a request, the request accompanied by a purchase price offer for the personal data. Further, and referring to the above description of Kepecs, it is indicated that the DAP computer which maintains the KEY database is networked to other computers which would include contact information. Therefore, it is apparent that Kepecs provides an ability to accept some contact information, as contact information in a profile as described in the specification of the pending application includes at least one of name, address, Social Security number and telephone number. Further, in the embodiment, where the consumer is supposedly "completely anonymous", Kepecs states that such a KEY has non-anonymous bindings elsewhere, presumably to store computer systems and computers of financial institutions where the consumers maintain accounts which by their very nature would include contact information. Non-anonymous bindings implies an ability to accept contact information.

Applicant therefore respectfully suggests that maintaining a KEY in a computer system that is linked to other computer systems which include and maintain contact information is separate and patentably distinct from an inability to accept contact information, as is recited in presently pending Claim 1. For the reasons set forth above, Claim 1 is submitted to be patentable over Goldhaber et al. in view of Kepecs.

Claims 3-7 depend from independent Claim 1. When the recitations of Claims 3-7 are considered in combination with the recitations of Claim 1, Applicant submits that dependent Claims 3-7 likewise are patentable over Goldhaber et al. in view of Kepecs.

Independent Claim 8 recites a method for providing advertising feedback, said method comprising the steps of "administering to each individual a password, absent any contact information for the individual," "utilizing the password to access a database," "entering profile information for the individual in the database," "maintaining the anonymity of the individual through an inability to accept contact information in the profile," "storing the entered profile information in the database," "presenting at least one of the individuals with a set of data," "receiving feedback from the at least one individual regarding the set of data" and "compensating the at least one individual for the feedback."

Goldhaber et al. in view of Kepecs do not describe nor suggest a method for creating an anonymous profile for an individual that includes "an inability to accept contact information". For example, Goldhaber et al. describe a system which requires both personal data (contact information) and profile data to be entered by a user. In addition, Goldhaber et al. describe that the personal data can be obtained by outside entities, should the member agree to a request, the request accompanied by a purchase price offer for the personal data. Further, and referring to the above description of Kepecs, it is indicated that the DAP computer which maintains the KEY database is networked to other computers which would include contact information. Therefore, it is apparent that Kepecs provides an ability to accept some contact information, as contact information in a profile as described in the specification of the pending application includes at

least name, address, Social Security number and telephone number. Further, in the embodiment, where the consumer is supposedly "completely anonymous", Kepecs states that such a KEY has non-anonymous bindings elsewhere, presumably to store computer systems and computers of financial institutions where the consumers maintain accounts which by their very nature would include contact information. Non-anonymous bindings implies an ability to accept contact information.

While, both Goldhaber et al. and Kepecs attempt to protect contact information, it appears that neither possess an inability to accept contact information. The selection of only a KEY with no other identification data does not imply an inability to accept contact information. It appears that the system of Kepecs does have an ability to accept contact information by virtue of the ability to accept the personal information listed above. The disclosure of Kepecs certainly describes a computer that attempts to maintain anonymity, through utilization of the stand-alone KEY, but admits that such computer maintains non-anonymous bindings utilizing the KEY to identify the consumer to other computers as above described. Further, in the embodiment where the KEY is utilized alone, it appears to be the choice of the consumer to utilize the KEY solely, and not an implementation of a method which includes an inability to accept contact information.

Applicant therefore respectfully suggests an inability to accept contact information, as is recited in presently pending Claim 8, is separate and patentably distinct from the KEY described in Kepecs. For the reasons set forth above, Claim 8 is submitted to be patentable over Goldhaber et al. in view of Kepecs.

Claims 9-15 depend from independent Claim 8. When the recitations of Claims 9-15 are considered in combination with the recitations of Claim 8, Applicant submits that dependent Claims 9-15 likewise are patentable over Goldhaber et al. in view of Kepecs.

Claim 16 recites an apparatus for conveying and storing information relating to anonymous data profiles. The apparatus includes "a first data repository," "a first computer linked to said first data repository, said first computer configured to communicate with said first

data repository via a password and provide a first set of information about an individual to said first data repository, the first set of information lacking information relating to a name, an address, a telephone number, and a social security number of the individual through an inability to accept contact information into said first computer" and "a processor programmed to communicate with said first data repository and said first computer". The apparatus further includes "a second data repository" and "a second set of computers linked to said second data repository, said second set of computers configured to provide a plurality of second sets of information to said second data repository, said first data repository separate from said second data repository, said processor further programmed to communicate with said second data repository and said second set of computers, said processor also programmed to receive and store feedback regarding the second sets of information, and provide compensation data to said first data depository and linked to the first information sets".

Goldhaber et al. in view of Kepecs do not teach nor suggest an apparatus which includes a first and second data repository which lacks information relating to a name, and address, a telephone number, and a social security number for an individual. Further, Goldhaber et al. in view of Kepecs do not teach nor suggest an inability to accept contact information into a computer. Rather, Goldhaber et al. in view of Kepecs describe a system which includes both personal data (contact information) and profile data. See Kepecs Column 6, lines 22-31. In addition, Goldhaber et al. describe that personal data (i.e. name, address, telephone) can be obtained by outside entities, should the member agree to a request, the request accompanied by a purchase price offer for the personal data. Kepecs describes a system where a database may include personal identification information, for example, mailing address, social security numbers, drivers license number and passport numbers, although Kepecs does describe not maintaining the contact information.

While, both Goldhaber et al. and Kepecs attempt to protect contact information, it appears that neither possess an inability to accept contact information. The selection of only a KEY with no other identification data does not imply an inability to accept contact information.

It appears that the system of Kepecs does have an ability to accept contact information by virtue of the ability to accept the personal information listed above. The disclosure of Kepecs certainly describes a computer that attempts to maintain anonymity, through utilization of the stand-alone KEY, but admits that such computer maintains non-anonymous bindings utilizing the KEY to identify the consumer to other computers as above described. Non-anonymous bindings implies an ability to accept contact information. Further, in the embodiment where the KEY is utilized alone, it appears to be the choice of the consumer to utilize the KEY solely, and not an implementation of an apparatus that embodies an inability to accept contact information.

The apparatus suggested by Goldhaber et al. in view of Kepecs would appear to be not maintaining direct consumer identification in the consumer account, as described at Column 2, lines 49-51. Applicant respectfully submits that "not maintaining" consumer identifications does not imply an inability to accept contact information. Therefore, Goldhaber et al. in view of Kepecs do not describe nor suggest any system or method which includes refusing to accept contact information from an individual. Therefore, neither Goldhaber et al., nor Kepecs, or the combination of the two, suggest an inability to accept contact information.

Further, Applicant respectfully suggests that Goldhaber et al. in view of Kepecs teach away from the apparatus recited in Claim 16 since Goldhaber et al. recite that an advertiser may pay for consumer names and addresses and Kepecs states that mailing address, social security numbers, and passport numbers are part of the database. Whereas in pending Claim 16, it is recited that information relating to names, addresses, telephone numbers, or social security numbers cannot be accepted into the system. For the reasons set forth above, Claim 16 is submitted to be patentable over Goldhaber et al. in view of Kepecs.

Claims 17 and 19-21 depend from independent Claim 16. When the recitations of Claims 17 and 19-21 are considered in combination with the recitations of Claim 16, Applicant submits that dependent Claims 17 and 19-21 likewise are patentable over Goldhaber et al. in view of Kepecs.

Independent Claim 22 recites a system for generating advertising feedback from anonymous consumers via an electronic data communications network. The system comprises "a control unit for coupling to the communications network," "a server coupled to said control unit and comprising a consumer generated data base for storing profile information relating to consumers, the data base having an inability to accept contact information within the profile, a marketer data base for storing information to be reviewed by consumers," and a processor programmed to "receive consumer generated data sets from consumers, said consumer generated data sets controlled by the consumers, each consumer generated data set including a set of individual characteristics, though refusing a name, an address, and a social security number entry for the consumer, said processor further programmed to download said consumer generated data sets into said consumer generated data base," "receive information from marketers, said information controlled by said marketers, said processor further programmed to download said marketer generated data into said marketer data base," "said processor further programmed to compare said marketer generated data to each said consumer generated data set and if said marketer generated data is identified as matching one or more said individual characteristics of said consumer generated data sets, designating said marketer generated data for being communicated to the consumer, said processor also programmed to receive feedback from the anonymous consumers regarding the marketer generated data, said system configured to provide compensation to the anonymous consumers for the feedback."

Goldhaber et al. in view of Kepecs do not teach nor suggest a system which is programmed to build data sets as described in Claim 22. Rather, Goldhaber et al. describe a system which includes both personal data (contact information) and profile data, albeit stored in different databases. In addition, Applicant respectfully suggests that Goldhaber et al. teach away from the methods recited in Claim 22 since Goldhaber et al. explains that a user is required to enter contact information (i.e. names, addresses, etc.) and that an advertiser may pay for consumer names and addresses. In pending Claim 22, it is explicitly stated that the consumer generated data sets do not include names, addresses, or social security numbers, since the

processor is programmed to refuse such entries. Kepecs describes a system having a database that may include personal identification information, for example, mailing address, social security numbers, drivers license number and passport numbers, although Kepecs does describe not maintaining the contact information.

While, both Goldhaber et al. and Kepecs attempt to protect contact information, it appears that neither possess an inability to accept contact information. The selection of only a KEY with no other identification data does not imply an inability to accept contact information. It appears that the system of Kepecs does have an ability to accept contact information by virtue of the ability to accept the personal information listed above. The disclosure of Kepecs certainly describes a computer that attempts to maintain anonymity, through utilization of the stand-alone KEY, but admits that such computer maintains non-anonymous bindings utilizing the KEY to identify the consumer to other computers as above described. Non-anonymous bindings implies an ability to accept contact information. Further, in the embodiment where the KEY is utilized alone, it appears to be the choice of the consumer to utilize the KEY solely, and not an implementation of an apparatus that embodies an inability to accept contact information.

The apparatus suggested by Goldhaber et al. in view of Kepecs would appear to be not maintaining direct consumer identification in the consumer account, as described at Column 2, lines 49-51. Applicant respectfully submits that "not maintaining" consumer identifications does not imply implies an inability to accept contact information. Therefore, Goldhaber et al. in view of Kepecs do not describe nor suggest any system or method which includes refusing to accept contact information from an individual. Therefore, neither Goldhaber et al., nor Kepecs, or the combination of the two, suggest an inability to accept contact information. For the reasons set forth above, Claim 22 is submitted to be patentable over Goldhaber et al. in view of Kepecs.

Claims 23-26 and 28 depend, directly or indirectly, from independent Claim 22. When the recitations of Claims 23-26 and 28 are considered in combination with the recitations of

Claim 22, Applicant submits that dependent Claims 23-26 and 28 likewise are patentable over Goldhaber et al. in view of Kepecs.

In additions to the reasons given above, Applicant respectfully submits that obviousness cannot be established by merely suggesting that it would have been obvious to one of ordinary skill in the art to modify Goldhaber et al. with Kepecs to produce the claimed invention. Rather, each allegation of what would have been an obvious matter of design choice must always be supported by citation to some reference work recognized as standard in the pertinent art, and the Applicant given an opportunity to challenge the correctness of the assertion or the repute of the cited reference. Applicant has not been provided with the citation to any reference supporting the assertions made in the rejection. Further, and to the extent understood, Goldhaber et al. in view of Kepecs do not describe or suggest the claimed combination, provide any motivation towards the claimed combination, and in fact teach away from the presently pending claims, since Goldhaber et al. require entry of contact information. Therefore Applicant respectfully submits that the presently pending claims are patentably distinguishable from the cited references.

For the reasons set forth above, Applicant respectfully requests that the Section 103 rejection of Claims 1, 3-17, 19-26, and 28 be withdrawn.

In view of the foregoing amendments and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,

Robert E. Slenker
Registration No. 45,112
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070